(Eddie) Jae K. Kim (CA 236805)
ekim@carlsonlynch.com
CARLSON LYNCH, LLP
1350 Columbia St. Ste. 603
San Diego, California 92101
Tel: (619) 762-1900
Fax: (619) 756-6991

Gary F. Lynch (to be admitted *pro hac vice*)
glynch@carlsonlynch.com
Kelly K. Iverson (to be admitted *pro hac vice*)
kiverson@carlsonlynch.com
CARLSON LYNCH, LLP
1133 Penn Avenue, Fl. 5
Pittsburgh, Pennsylvania 15222
Tel: (412) 322-9243
Fax: (412) 231-0246

Attorneys for Plaintiff Addi Jadin and the Putative Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ADDI JADIN, individually, and on behalf of all others similarly situated,

Plaintiff,

v.

HANNA ANDERSSON, LLC; SALESFORCE.COM, INC.;

Defendants.

Case No.:

CLASS ACTION COMPLAINT FOR:

(1) Negligence;

(2) Negligence per se; and

(3) Violation of the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200).

DEMAND FOR JURY TRIAL

Plaintiff Addi Jadin ("Plaintiff"), by her attorneys, hereby brings this class and representative action against Hanna Andersson, LLC ("Hanna") and Salesforce.com, Inc. ("Salesforce" and, collectively with Hanna, "Defendants").

NATURE OF THE ACTION

1. All allegations herein are based upon information and belief except those allegations which pertain to Plaintiff or her counsel. Allegations pertaining to Plaintiff or her counsel are based upon, inter alia, Plaintiff or her counsel's personal knowledge, as well as Plaintiff or her counsel's own investigation. Furthermore, each allegation alleged herein either has evidentiary support or is likely to have evidentiary support, after a reasonable opportunity for additional investigation or discovery.

2. This is a class and representative action brought by Plaintiff to assert claims in her own right, and in her capacity as the class representative of all others persons similarly situated, and in her capacity as a private attorney general on behalf of the members of the general public. Defendants wrongfully exposed and permitted the exfiltration and theft of comprehensive financial and personally identifiable information ("PII") of Plaintiff and the class members through Defendants' negligent, inadequate, and unreasonable data security policies and practices. Plaintiff, on behalf of herself and the class assert claims of negligence and violation of the California Unfair Competition Laws, Bus. & Prof. Code § 7200, *et seq*.

PARTIES

3. Plaintiff is a resident of Bozeman, Montana, and, at all relevant times, has been a customer of Hanna, which used Salesforce's e-commerce platform to process transactions and store customer data.

4. Defendant Hanna Andersson, LLC is retailer of children's apparel that is incorporated in Delaware, with its principal place of business located at 1010 Northwest Flanders street, Portland, Oregon. During the class period, Hanna operated in California through its website and six (6) stores in California, including in Palo Alto, Walnut Creek, and Livermore, and contracted with Salesforce to provide its ecommerce platform from California.

5. Defendant Salesforce.com, Inc. is a provider of a cloud-base ecommerce platform that is incorporated in Delaware with its principal place of business located at 1 Market Street, San Francisco, California. During the class period, Salesforce provided the ecommerce platform Salesforce Commerce Cloud Unit to Hanna for processing customers' online sales transactions and data.

VENUE AND JURISDICTION

6. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because: (1) the claims of plaintiffs aggregated together exceed $5,000,000, and (2) some putative class members are residents of different states than Defendant.

7. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant Salesforce.com, Inc., is headquartered in this District, Defendant Hanna does business in this District,

and a substantial part of the events and/or omissions giving rise to the claims asserted herein occurred in or were directed from this District.

FACTUAL ALLEGATIONS

A. Defendant's Negligent, Inadequate and Unreasonable Security Policies and Procedures

8. Hanna is a retail corporation that specializes in children's apparel and accessories with over 60 retail locations throughout the United States and with annual revenues exceeding $140 million. It also sells merchandise through its online store at www.hannaandersson.com.

9. Salesforce is a software company that sells, provides and maintains cloud-based ecommerce platforms, including the Salesforce Commerce Cloud utilized by Hanna, through which retailers can establish websites, advertise, sell goods and services, process transactions, and maintain data. The Salesforce Commerce Cloud platform is currently used by over 3,000 live websites,[1] and recently announced its revenue for the third quarter of 2019 of $4.5 billion, up 33% year-over-year.[2]

10. In order to process online sales transactions, Salesforce's platform requires customers to input various personal and payment information.

11. Salesforce represents and markets the strength of the security procedures and policies in place to protect data that is processed and stored in its cloud platform by stating:

a. "Salesforce, the leading authority in cloud-based CRM [customer relations management], recognizes the need for a secure cloud. To provide clients with the most secure solutions possible, Salesforce incorporates a range of security tools into every service they provide. In fact, Salesforce provides a community hub for real-time data on Salesforce performance and security, in the form of Salesforce Trust."

b. "Salesforce Trust is a website that gives [users] access to the security status of every Salesforce platform, so they can see at a glance how protected their data is. Service availability, privacy, compliance, and security are all presented with total transparency. Essentially, with Salesforce, trust is built right in."[3]

[1] https://trends.builtwith.com/shop/Salesforce-Commerce-Cloud

[2] https://investor.salesforce.com/press-releases/press-release-details/2019/Salesforce-Announces-Record-Third-Quarter-Fiscal-2020-Results/default.aspx

[3] https://www.salesforce.com/products/platform/best-practices/improving-cloud-security/

c. "Salesforce, the leading authority in cloud-based CRM, recognizes the need for a secure cloud. To provide clients with the most secure solutions possible, Salesforce incorporates a range of security tools into every service they provide. In fact, Salesforce provides a community hub for real-time data on Salesforce system performance and security, in the form of Salesforce Trust."

d. "Salesforce Trust is a website that gives uses access to the security status of every Salesforce platform, so they can see at a glance how protected their data is. Service availability, privacy, compliance, and security are all presented with total transparency. Essentially, with Salesforce, trust is built right in."[4]

e. "Security protocols and infrastructure are constantly analyzed and updated to address new threats."

f. Some of the world's largest companies moved their applications to the cloud with Salesforce after rigorously testing the security and reliability of our infrastructure."

g. "The cloud is used to back up data, deliver, software, and provide extra processing capacity in a secure, scalable way."

h. "[C]loud data is probably more secure than information stored on conventional hard drives."

i. "With cloud services, information is encrypted and backed up continuously. Vendors monitor systems carefully for security vulnerabilities."

j. "With PaaS, the vendor takes care of back-end concerns such as security, infrastructure, and data integration so users can focus on building, hosting, and testing apps faster and at lower cost."[5]

12. Hanna also touts its strong security measures:

> The security of your personal information is very important to Hanna, and we have implemented measures to ensure your information is processed confidentially, accurately, and securely. Our website is PCI DSS complaint and uses SSL/TLS (Secure Sockets Layer) technology to encrypt your order information, such as your name, address, and

[4] https://www.salesforce.com/products/platform/best-practices/improving-cloud-security/

[5] https://www.salesforce.com/products/platform/best-practices/cloud-computing/

> credit card number, during data transmission. We use a third party payment processor, which is also PCI DSS compliant."[6]

13. The Payment Card Industry Data Security Standard ("PCI DSS") is an information security standard for organizations that handle branded credit cards and is mandated by the card brands (i.e., Visa, MasterCard, etc.) and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud and protect customer data. Some of the requirements included installing and maintaining a firewall configuration to protect cardholder data; protecting stored cardholder data through encryption, hashing, masking, and truncation; encrypting transmission of cardholder data over open, public networks; protecting all systems against malware and performing regular updates of anti-virus software to reduce the risk of exploitation via malware; developing and maintaining secure systems and applications, including immediately installing security patches to fix vulnerability and prevent exploitation and compromise of cardholder data; and testing security systems and processes regularly.[7]

14. To purchase items on Hanna's website, customers are required, at a minimum, to enter the following PII onto the website: (a) name; (b) billing address; (c) shipping address; (d) telephone number; (e) email address; (f) name on the credit card; (g) type of credit card; (h) full credit card number; (i) credit card expiration date; and (j) security CVV code.

B. The Breach

15. On or about January 15, 2020, Hanna sent customers a *Notice of Security Incident* ("Customer Notice"). In this Customer Notice, Hanna stated that "[l]aw enforcement recently notified Hanna Andersson that it had obtained evidence indicating that an unauthorized third party had accessed information entered on Hanna Andersson's website during purchases made between September 16 and November 11, 2019…. The incident potentially involved information submitted during the final purchase process on our website, www.hannaandersson.com, including name, shipping address, billing address, payment card number, CVV code, and expiration date."[8]

---

[6] https://www.hannaandersson.com/security-and-privacy.html

[7] https://www.pcisecuritystandards.org/

[8] https://media.dojmt.gov/wp-content/uploads/Breach-NotificationDetails-98.pdf; https://oag.ca.gov/system/files/Hanna_Multi-State%20Master__Rev1.pdf

16. On that same day, January 15, 2020, Hanna's counsel mailed a different *Notification of Security Incident* to the Attorney General of states throughout the country ("AG Notice"). Curiously, the AG Notice provided additional as well as conflicting information to the Customer Notice.

17. Piecing together the information provided by Hanna's Customer Notice and AG Notice—which is the entirety of the information that either Hanna or Salesforce has provided—reveals inconsistencies and questionable and problematic decision-making that have substantially increased the exposure and harm to customers:

a. **September 16, 2019**: The earliest potential date of compromise identified by forensic investigators, according to the AG Notice. At some point after this date, credit cards used on Hanna's website became available for purchase on a "dark web" site. The information that was scraped may have included name, billing and shipping address, payment card number, CVV code, and expiration date. The fact that the PII is available for purchase on the dark web indicates that the PII was not protected with sufficient and adequate encryption.

b. **November 11, 2019**: The malware was removed, according to the AG Notice. There is no explanation of how the malware could have been removed when Hanna claims that it was not aware of the existence of the malware and breach until law enforcement notified Hanna on December 5, 2019 (see below). There is no indication of whether Salesforce was aware of the breach, exfiltration and theft of customers' personal and financial data prior to November 11, 2019, in order to remove the malware on its Commerce Cloud platform, nor any indication that Salesforce ever informed Hanna of the breach, exfiltration and theft of its customers' data from Salesforce's ecommerce platform. It appears improbable the malware on Salesforce's ecommerce platform was removed without Defendants (or at least Salesforce) being aware of it. The notices imply that Salesforce itself never provided notice to attorneys general or Hanna's customers of the breach of their data.

c. **December 5, 2019**: Law enforcement informed Hanna that credit cards used on its website were available for purchase on a dark web site, according to the AG Notice. Hanna immediately launched an investigation which confirmed that Hanna's third-party ecommerce platform, Salesforce Commerce Cloud, was infected with malware that may have scraped

information entered by customers into the platform during the purchase process. Meanwhile, in the Customer Notice, Hanna describes the timing of when it was notified by law enforcement of the breach as being "recently" prior to mailing out the Customer Notice on January 15, 2020, and never mentions the December 5, 2019 date of being notified by law enforcement.

d. **December 31, 2020**: Hanna determined that it would notify customers who made purchases on its website during the relevant timeframe that they may have been impacted by the breach, and the notice was disseminated over two weeks later on January 15, 2020, according to the AG Notice. There is no indication that law enforcement requested that Hanna hold off on providing notice to customers and attorneys general until January 15, 2020, and no indication that law enforcement requested that Salesforce not provide any notice at all to customers and attorneys general.

e. **January 15, 2020**: The AG Notice and Customer Notice were mailed and posted. Meanwhile, the comprehensive set of customers' financial and personal identifying information had already been available for purchase on the dark web for four months before customers were made aware of the breach, exfiltration, and theft of their information.

18. In the type of attack that occurred here—dubbed "Magecart"—threat actors hack into vulnerable ecommerce platforms used by online stores and inject malicious scripts into checkout pages. The scripts, known as web skimmers or scrapers, are then used to collect the customers' payment info and send it to attacker-controlled remote sites. The groups behind Magecart attacks have been active since at least 2010, according to a RiskIQ report, and they are known to target online stores that use ecommerce platforms such as Magento, OpenCart, PrismWeb, and OSCommerce.[9]

19. In fact, during the time that Defendants' customers' data was being scraped, the FBI's office in Portland, Oregon, which is the city where Hanna is based, issued a publication entitled *Oregon FBI Tech Tuesday: Building a Digital Defense Against E-Skimming* on October 22, 2010, wherein the agency warned:

a. "This warning is specifically targeted to … businesses… that take credit card payments online. E-skimming occurs when cyber criminals inject malicious code onto a website.

[9] https://www.bleepingcomputer.com/news/security/us-retailer-hanna-andersson-hacked-to-steal-credit-cards/

The bad actor may have gained access via a phishing attach targeting your employees – or through a vulnerable third-party vendor attached to your company's server.

b. "Here's what businesses and agencies can do to protect themselves:

- Update and patch all systems with the latest security software. Anti-virus and anti-malware need to be up-to-date and firewalls strong.
- Change default login credentials on all systems.
- Educate employees about safe cyber practices. Most importantly, do not click on links or unexpected attachments in messages.
- Segregate and segment network systems to limit how easily cyber criminals can move from one to another."[10]

20. Based on widely publicized prior attacks to ecommerce cloud platforms, the prescriptions of the PCI DSS, and the warnings set forth by the FBI, Defendants had sufficient knowledge to reasonably foresee the harm caused to customers by utilizing inadequate and unreasonable security measures to protect their PII, but failed to act reasonably. Furthermore, Defendants' actions and non-actions during and after the data breach—in particular their belated, inadequate, and conflicting notice to customers—likely caused customers additional, avoidable harm.

21. Defendants knew and should have known that failure to maintain adequate technological safeguards would eventually result in a significant data breach, exposing its customers' card numbers to hackers. Defendants could have and should have substantially increased the amount of money they spent to protect against cyber-attacks but chose not to. Plaintiff and the Class should not have to bear the expense caused by Defendants' negligent failure to safeguard their financial and personal identifying information form cyber-attackers.

C. Plaintiff's Experience

22. Plaintiff Addi Jadin purchased products from Hanna's online store at www.hannandersson.com between September 16 and November 11, 2019. On the payment platform on Hanna's online store that is processed by Salesforce's ecommerce platform, Plaintiff entered her name,

[10] https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-agaist-e-skimming

billing and shipping addresses, payment card type and full number, CVV code, credit card expiration date, and email address.

23. Plaintiff received Hanna's January 15, 2020 Customer Notice, but did not receive Hanna's AG Notice, nor any sort of notice at all from Salesforce.

24. As a result of the breach, exfiltration and theft of her financial and PII, Plaintiff has expended her time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the future consequences of the data breach, including investigating the information compromised and how best to ensure she is protected from potential identity theft, which efforts are continuous and ongoing.

25. Plaintiff has also suffered injury directly and proximately caused by the data breach including: (a) theft of her valuable PII; (b) the imminent and certain impeding injury flowing from fraud and identity theft posed by her PII being placed in the hands of criminals; (c) damages to and diminution in value of their PII that was entrusted to Defendants with the understanding Defendants would safeguard the PII against disclosure; (d) loss of the benefit of the bargain with Defendants to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff should have received from Defendants when Defendants represented Plaintiff's PII would be protected by reasonable data security, and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; and (e) continued risk to Plaintiff's PII, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate an adequate measures to protect the PII that was entrusted to Defendants.

CLASS ACTION ALLEGATIONS

26. The preceding allegations are incorporated by reference and re-alleged as if fully set forth herein.

27. Plaintiff brings this case, and each of her respective causes of action, as a class action pursuant to Federal Rule of Civil Procedure 23(a)(b)(1), (b)(2) and (b)(3) on behalf of the following class.

28. The "Class" is composed of: **All individuals whose PII was compromised in the data breach announced by Hanna Andersson on or about January 15, 2020**.

29. Excluded from the Class is: (1) any entity in which a Defendant has a controlling interest; (2) officers or directors of a Defendant; (3) this Court and any of its employees assigned to work on the case; and (4) all employees of the law firms representing Plaintiff and the Class members.

30. This action has been brought and may be properly maintained on behalf of each member of the Class under Federal Rule of Civil Procedure 23.

31. **Numerosity of the Class (Federal Rule of Civil Procedure 23(a)(1))** – The members of the Class are so numerous that a joinder of all members would be impracticable. While the exact number of Class members is presently unknown to Plaintiff, and can only be determined through appropriate discovery, Plaintiff believes that the Class is likely to include thousands of members based on the fact that Hanna has approximately $140 million in assets and sells items through its online store throughout the United States.

32. Upon information and belief, Defendants have databases, and/or other documentation, of its customers' transactions. These databases and/or documents can be analyzed by an expert to ascertain which of Hanna's customers have been harmed by Defendants' policies and practices and thus qualify as Class members. Further, the Class definition identifies groups of unnamed plaintiffs by describing a set of common characteristics sufficient to allow a member of that group to identify himself or herself as having a right to recover. Other than by direct notice by mail or email, alternatively proper and sufficient notice of this action may be provided to the Class members through notice published in newspapers or other publications.

33. **Commonality (Federal Rule of Civil Procedure 23(a)(2))** – This action involves common questions of law and fact. The questions of law and fact common to both Plaintiff and the Class members include, but are not limited to, the following:

a. whether Defendants owed a legal duty to Plaintiff and the Class members to exercise reasonable care in collecting, storing, using, and safeguarding their PII;

b. whether Defendants breached a legal duty to Plaintiff and the Class members to exercise reasonable care in collecting, storing, using and safeguarding their PII;

c. whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach; and

e. whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

34. **Typicality (Federal Rule of Civil Procedure 23(a)(3))** – Plaintiff's claims are typical of all of the members of the Class. The evidence and the legal theories regarding Defendant's alleged wrongful conduct committed against Plaintiff and all of the Class members are substantially the same. Plaintiff's claim is typical of the Class's claims in that they all involve the same types of online transactions and utilized the same platform; the type of PII that was subject to the data breach and theft is the same; and the forms of harm suffered by Plaintiff and the Class are of the same character. Accordingly, in pursuing her own self-interest in litigating her claims, Plaintiff will also serve the interests of the other Class members.

35. **Adequacy (Federal Rule of Civil Procedure 23(a)(4))** – Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff has retained competent counsel experienced in class action litigation to ensure such protection. There are no material conflicts between the claims of the representative Plaintiff and the members of the Class that would make class certification inappropriate. Plaintiff and her counsel intend to prosecute this action vigorously.

36. **Predominance and Superiority (Federal Rule of Civil Procedure 23(b)(3))** – The matter is properly maintained as a class action under Rule 23(b)(3) because the common questions of law or fact identified herein and to be identified through discovery predominate over questions that may affect only individual Class members. Further, the class action is superior to all other available methods for the fair and efficient adjudication of this matter. Because the injuries suffered by the individual Class members are relatively small, the expense and burden of individual litigation would make it virtually impossible for Plaintiff and Class members to individually seek redress for Defendants' wrongful conduct. Even if any individual person or group(s) of Class members could afford individual

litigation, it would be unduly burdensome to the courts in which the individual litigation would proceed. The class action device is preferable to individual litigation because it provides the benefits of unitary adjudication, economies of scale, and comprehensive adjudication by a single court. In contrast, the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for the party (or parties) opposing the Class and would lead to repetitious trials of the numerous common questions of fact and law. Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action. As a result, a class action is superior to other available methods for the fair and efficient adjudication of this controversy. Absent a class action, Plaintiff and the Class members will continue to suffer losses, thereby allowing Defendants' violations of law to go without remedy.

37. Plaintiff anticipates the issuance of notice, setting forth the subject and nature of the instant action, to the proposed Class members. Upon information and belief, Defendants' own business records and/or electronic media can be utilized for the contemplated notices. To the extent that any further notices may be required, Plaintiff anticipates the use of additional media and/or mailings.

38. This matter is properly maintained as a class action pursuant to Rule 23(b) of the Federal Rules of Civil Procedure, in that:

a. Without class certification and determination of declaratory, injunctive, statutory and other legal questions within the Class format, prosecution of separate actions by individual members of the Class will create the risk of:

i. inconsistent or varying adjudications with respect to individual members of the Class which would establish incompatible standards of conduct for the parties opposing the Class; or

ii. adjudication with respect to individual members of the Class, which would as a practical matter be dispositive of the interests of the other members not parties to the adjudication or substantially impair or impede their ability to protect their interests. The parties opposing the Class have acted or refused to act on grounds generally applicable to each member of the Class,

thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

b. Common questions of law and fact exist as to the members of the Class and predominate over any questions affecting only individual members, and a class action is superior to other available methods of the fair and efficient adjudication of the controversy, including consideration of:

i. the interests of the members of the Class in individually controlling the prosecution or defense of separate actions;

ii. the extent and nature of any litigation concerning controversy already commenced by or against members of the Class;

iii. the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and

iv. the difficulties likely to be encountered in the management of a class action.

FIRST CAUSE OF ACTION

Negligence

(Against All Defendants)

39. The preceding allegations are incorporated by reference and re-alleged as if fully set forth herein.

40. At all relevant times, Defendants were under a duty to act with reasonable care in the collection and processing of Plaintiff and the Class's PII. Defendants undertook care of PII belonging to Plaintiff and the Class members, then breached their legal duty by failing to maintain adequate technological safeguards, falling below the standard of care in the technological industry, directly and proximately causing foreseeable risk of data loss and credit harm and identity theft and other economic losses, in amounts to be decided by the jury. Defendants' failure to comply with laws requiring it to notify consumers of its data breach in the most expeditious manner possible also constitutes negligence.

41. As a result of Defendants' negligence, Plaintiff and Class members suffered injuries that may include: (1) the lost or diminished value of PII; (2) out-of-pocket expenses associated with the

prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of the PII; (3) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (4) the continued risk to their PII, which remains for sale on the dark web and is in Defendants' possession, subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; (5) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiff and Class members, including ongoing credit monitoring.

42. These injuries were reasonably foreseeable given the history of security breaches of this nature.

43. The injury and harm that Plaintiff and the other Class members suffered was a direct and proximate result of Defendants' negligent conduct.

SECOND CAUSE OF ACTION

Negligence Per Se

(Against All Defendants)

44. The preceding allegations are incorporated by reference and re-alleged as if fully set forth herein.

45. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which prohibits "unfair… practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Defendants.

46. Defendants violated Section 5 of the FTC Act (and similar state statutes, such as Cal. Civ. Code § 1798.81.5) by mishandling Plaintiff's and the Class members' personal information, failing to use reasonable measures to protect the personal information, and by not complying with applicable industry standards.

47. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

48. Plaintiff and the Class are within the scope of persons that Section 5 of the FTC Act (and similar state statutes) was intended to protect.

49. Furthermore, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class here.

50. As a direct and proximate result of Defendants' negligence per se, Plaintiff and the Class have suffered and continue to suffer injury and damages, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the data breach; theft of their valuable PII; the imminent and certain impeding injury flowing from fraud and identity theft posed by their PII being placed in the hands of hackers; damages to and diminution in value of their PII that was entrusted to Defendants for the sole purpose of obtaining products through Defendants' website and ecommerce platform with the understanding that Defendants would safeguard the PII against disclosure; and continued risk to Plaintiff's and the Class members' PII, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fails to undertake appropriate an adequate measures to protect the PII that was entrusted to Defendants.

THIRD CAUSE OF ACTION

For Violation of the California Unfair Competition Law

(Against Defendant Salesforce.com)

51. The preceding allegations are incorporated by reference and realleged as if fully set forth herein.

52. Plaintiff, who has suffered injury in fact and has lost money or property as a result of Defendants' violations of the California Unfair Competition Law, Business and Professions Code §§ 17200 *et. seq*., alleges this cause of action as a class action and as a private attorney general on behalf of the members of the general public.

53. Defendants have engaged in, and continue to engage in, general business practices of implementing and utilizing inadequate and unreasonable data security measures to protect their customers' PII and failure to act timely to remediate the breach and provide timely and adequate notice of the breach in order to reduce the amount of future harm to customers. Indeed, Salesforce has failed to provide any notice whatsoever.

54. These failures contravene the public policies set forth in California Civil Code § 1798.81.5 and the FCTA Act. Defendants' actions were negligent, knowing and willful, and /or wanton and reckless with respect to the rights of Plaintiff and Class members.

55. Defendants' practices are also unfair since they have no utility and, even if they did, any utility is outweighed by the gravity of harm to Plaintiff and the Class members. Defendants' practices are also immoral, unethical, oppressive or unscrupulous and cause injury to consumers which outweigh their benefits.

56. By reason of the foregoing, Defendants have been improperly and unjustly enriched to the detriment of Plaintiff and the Class members in an amount to be proven at trial. Plaintiff and the Class members are entitled to have Defendants disgorge and restore to Plaintiff and the Class members all monies wrongfully obtained by Defendants as a result of their conduct as alleged herein.

57. Unless Defendants are enjoined from continuing to engage in these business practices, Plaintiff and the Class members will continue to be injured by Defendants' wrongful actions and conduct. Therefore, Plaintiff and the Class members are entitled to injunctive relief, including public injunctive relief.

PRAYER

WHEREFORE, Plaintiff and the Class pray for judgment as follows:

1. For an order certifying this action as a class action, and appointing Plaintiff and her Counsel to represent the Class;

2. For compensatory damages on all applicable claims and in an amount to be proven at trial;

3. For an order requiring Defendants to disgorge, restore, and return all monies wrongfully obtained together with interest calculated at the maximum legal rate;

4. For an order enjoining the wrongful conduct alleged herein, and instructing Defendants to implement proper security measures to remedy their security failures and to ensure that Plaintiff and the class are not subjected to any future theft of their PII due to Defendants' inadequate security measures. Such relief shall include issuance of public injunctive relief;

5. For costs;

6. For pre-judgment and post-judgment interest as provided by law;

7. For attorneys' fees under the common fund doctrine, California Code of Civil Procedure § 1021.5, and/or under all other applicable law; and

8. For such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff and the Class members demand a trial by jury on all issues so triable.

Dated: February 20, 2020

CARLSON LYNCH, LLP

/s/ (Eddie) Jae K. Kim

(Eddie) Jae K. Kim (CA 236805)
ekim@carlsonlynch.com
1350 Columbia St., Ste. 603
San Diego, California 92101
Tel.: 619.762.1900
Fax: 619.756.6991

Gary F. Lynch (to be admitted *pro hac vice*)
glynch@carlsonlynch.com
Kelly K. Iverson (to be admitted *pro hac vice*)
kiverson@carlsonlynch.com
CARLSON LYNCH, LLP
1133 Penn Avenue, Fl. 5
Pittsburgh, Pennsylvania 15222
Tel: (412) 322-9243
Fax: (412) 231-0246